

Page 12, after the last line, insert the following:

--I claim:--

IN THE CLAIMS

Please substitute amended claims 1-15 as presented below for the same-numbered claims that were pending prior to the filing of this paper. A marked-up version of the amended claims is attached.

10030255 010902

1 1. (Amended) A method for authenticating a portable object including
2 information processing means and information storage means, the information
3 storage means containing at least one code defining operation steps capable of
4 being executed by the portable object, as well as a one-way function, comprising
5 sending the portable object an order for executing a calculation of a result by
6 applying to said one-way function at least part of said code and using said result to
7 decide whether or not the portable object is authentic.

1 2. (Amended) A method according to claim 1, wherein said result enters
2 into the implementation of a predetermined operation, said operation being
3 performed successfully only when the portable object is authentic.

1 3. (Amended) A method according to claim 2, wherein said predetermined
2 operation comprises a decryption operation, said result making it possible to produce
3 an associated decryption key.

1 4. (Amended) A method according to claim 1, wherein said part of said
2 code used in the calculation, comprises a machine code.

1 5. (Amended) A method according to claim 1, wherein the portable object
2 contains a real code defining operations designed to be executed by the portable
3 object, and a dummy code defining operations not designed to be executed by the
4 portable object, said code used in the calculation of a result comprising a dummy
5 code.

1 6. (Amended) A method according to claim 1, further comprising
2 repeatedly sending said order to the portable object during its life, prior to execution
3 by the portable object of said operation steps.

1 7. (Amended) A method according to claim 1, wherein said code used in
2 the calculation is defined by a start address and an end address in the information
3 storage means, and further including the step of sending said start and end
4 addresses to the portable object.

1 8. (Amended) A method according to claim 1, wherein said code
2 comprises a set of binary words, said code used in the calculation being defined by a
3 subset of said binary words comprising binary words distributed in the information
4 storage means at a determined pitch, said pitch being sent to the portable object.

1 9. (Amended) A method for having a portable object execute a sensitive
2 operation, the portable object comprising information processing means and
3 information storage means, comprising: storing in the information storage means at
4 least one code defining operations capable of being executed by the portable object,
5 as well as a one-way function, and sending the portable object an order so that the
6 portable object executes a calculation of a result by applying to said one-way
7 function at least part of said code, said result entering into the implementation of said
8 sensitive operation, said operation being performed successfully only when the
9 portable object is authentic.

1 10. (Amended) A method according to claim 9, wherein the code part used
2 in the calculation comprises a machine code.

1 11. (Amended) A method according to claim 9, wherein the portable object
2 contains a real code defining operations designed to be executed by the portable
3 object, and a dummy code defining operations not designed to be executed by the
4 portable object, said code part used in the calculation comprising a dummy code.

1 12. (Amended) A portable object, comprising: information processing
2 means, information storage means, the information storage means containing at
3 least one code defining operations capable of being executed by the portable object,
4 as well as a one-way function, and means for executing a calculation of a result by
5 applying to said one-way function at least part of said code.

1 13. (Amended) A portable object according to claim 12, wherein said code
2 part used in the calculation comprises a machine code.

1 14. (Amended) A device comprising: information processing means,
2 information storage means, said information processing means designed to
3 communicate with a portable object in order to authenticate the portable object, the
4 portable object comprising: information processing means, information storage
5 means, the information storage means of the portable object containing at least one
6 code defining operations capable of being executed by the portable object, as well
7 as a one-way function, and means for sending the portable object an order so that

8 the portable object executes a calculation of a result by applying to said one-way
9 function at least part of said code of the portable object.

1 15. (Amended) A device according to claim 14, wherein said code part
2 used in the calculation comprises a machine code.

10030255-010902
205070" 55208001